PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-357126

(43)Date of publication of application : 26.12.2000

---

(51)Int.Cl. G06F 12/14

---

(21)Application number : 11-169980 (71)Applicant : TOSHIBA CORP
MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 16.06.1999 (72)Inventor : KAMIBAYASHI TATSU
YAMADA HISASHI
IWASAKI HIROSHI
TAMURA MASABUMI
ISHIBASHI YASUHIRO
KATO HIROSHI
TATEBAYASHI MAKOTO
HARADA TOSHIHARU
KATSUTA NOBORU

---

# (54) STORAGE MEDIUM AND CONTENTS PROTECTING METHOD USING THE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To protect contents by making illegal electronic equipment ineffective when a storage medium is mounted on the electronic equipment represented by revocation information and used by previously registering the revocation information

in a specific storage area of the storage medium.

SOLUTION: In a read-only open ROM area 132 secured on a PM (storage medium) 13, a revocation list RL by which a PD (recording and reproducing device) to be made ineffective for contents protection can be decided is previously registered and when the PM 13 is mounted on an LCM (contents use management system) or the PD and used, a controller 130 provided on the PM 13 receives information. representing the LCM or PD from the equipment, refers to the revocation list RL with the information, and determines whether or not the equipment is made ineffective according to the reference result.

---

LEGAL STATUS [Date of request for examination] 19.10.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

## CLAIMS

---

[Claim(s)]
[Claim 1] The storage characterized by to make nullification of the electronic equipment concerned controllable according to said RIBOKESHON information when the specific storage region where the RIBOKESHON information which is a storage available to the record or the playback of a digital content by the electronic equipment which has either [ at least ] the record function of a digital content or a regenerative function, and can distinguish the electronic equipment which should be cancelled for contents protection was registered beforehand provides and it uses it, being equipped the electronic equipment of arbitration with said storage.
[Claim 2] The storage according to claim 1 characterized by receiving the information showing the electronic equipment concerned from the electronic equipment concerned, and providing further the controller which controls nullification of the electronic equipment concerned by the information with reference to said RIBOKESHON information according to the reference result when using it, equipping the electronic equipment of arbitration with said storage.
[Claim 3] The storage according to claim 1 with which said specific storage region is characterized by being reserved storage on read-only nonvolatile memory.
[Claim 4] The storage according to claim 1 characterized by said specific storage region being a storage region which was secured on rewritable nonvolatile memory, and which cannot be accessed except the specific procedure kept secret.
[Claim 5] A specific storage region is established in a storage available to the record or playback of a digital content by the electronic equipment which has either [ at least ] the record function of a digital content, or a regenerative function. The RIBOKESHON information which can distinguish the electronic equipment which should be cancelled for contents protection is beforehand registered into the specific storage region concerned. The contents protection approach characterized by controlling nullification of the electronic equipment concerned according to said RIBOKESHON information when using it, equipping the electronic equipment of

arbitration with one of said the storages.

[Claim 6] A specific storage region is established in each of the storage with which the available storage media section and an available controller were united with the record or playback of a digital content by the electronic equipment which has either [ at least ] the record function of a digital content, or a regenerative function. To the specific storage region concerned The RIBOKESHON information which can distinguish the electronic equipment which should be cancelled for contents protection is registered beforehand. When using it, equipping the electronic equipment of arbitration with one of said the storages The contents protection approach characterized by receiving the information which expresses the electronic equipment concerned with said controller on the storage from the electronic equipment concerned, and controlling nullification of the electronic equipment concerned by the information with reference to said RIBOKESHON information according to the reference result.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the storage used for carrying out record playback of the various digital contents represented by image data and music data, and relates to the contents protection approach which used the suitable storage

to inhibit record playback of the contents by unjust electronic equipment especially, and this medium.

[0002]

[Description of the Prior Art] In recent years, various electronic equipment, such as a personal computer corresponding to multimedia, a set top box, a player, and a game machine, is developed with development of computer technology. This kind of electronic equipment can reproduce various digital contents, such as image data, music data, etc. which were stored in the archive medium, and also a digital content can also be downloaded and used for it through the Internet etc.

[0003] These digital contents can be copied by adoption of MPEG 2 and the digital coding technique of MP3, without lowering quality, or can be downloaded. For this reason, recently, the need for the technique for protecting such a digital content from an unauthorized use is cried for from a viewpoint of protection of copyrights.

[0004]

[Problem(s) to be Solved by the Invention] However, even if the storage used by electronic equipment, such as a personal computer, a set top box, and a player, moves to another device, there are many records / reproducible reversible things, and the specification is fundamentally open. For this reason, since migration/copy of contents can be performed freely, it is difficult to protect the contents memorized by the storage from unjust copy/migration in practice.

[0005] then, the specific procedure kept secret about the storage with which the storage media section and a controller were unified like a memory card — only — it is possible to aim at protection of contents by being able to access, preparing from a user the access impossible field (secrecy field) which cannot be accessed, and storing important information required for use of contents of copy control information, migration control information, etc. there.

[0006] in this case, in case copy/migration of contents are performed between electronic equipment, such as a personal computer, a set top box, and a player, and a storage It attests mutually whether it is the just thing which is sharing the predetermined structure (that is, predetermined contents protection feature) about protection of copyrights (contents protection), respectively. According to the algorithm of the key generation mutually shared when it is able to attest with the right, perform key exchange, and an authentication key common according to an individual is acquired. Using the authentication key for encryption (license encryption) / decryption of a contents key (key which enciphers contents), or encryption/decryption of contents is also considered.

[0007] However, the device which has this kind of problem only by the above-mentioned mutual recognition [ when it becomes what has the unnecessary structure of contents protection for example, by attack that the device (program which operates in a top) concerned is changed after the purchase of a device since information required for the above-mentioned mutual recognition is beforehand set up in the shipment phase of a device etc. ] can be detected [ . ].

[0008] This invention is what was made in consideration of the above-mentioned situation. The purpose By considering as the configuration in which the RIBOKESHON information which can distinguish the electronic equipment which should be cancelled for contents protection was beforehand registered into the specific storage region When using it, equipping the electronic equipment expressed with the RIBOKESHON information concerned, it is in offering the contents protection approach which used the storage which the electronic equipment is cancelled and can aim at protection of contents, and this medium.

[0009]

[Means for Solving the Problem] The storage of this invention is having the specific storage region where the RIBOKESHON information which can distinguish the electronic equipment which it is available to the record or the playback of a digital content by the electronic equipment which has either [ at least ] the record function of a digital content or a regenerative function, and should be cancelled for contents protection was registered beforehand, and when using it, being equipped the electronic equipment of arbitration with self, it is characterized by to make nullification of the electronic equipment concerned controllable according to the above-mentioned RIBOKESHON information.

[0010] Thus, it is considering as the configuration in which RIBOKESHON information's was beforehand registered into the specific storage region in the storage of this invention, and when using it, equipping the electronic equipment expressed with the RIBOKESHON information concerned, it becomes possible to cancel the electronic equipment and to aim at protection of contents.

[0011] A storage is considered as the configuration with which the storage media section and a controller were united like a memory card here. When using it, equipping the electronic equipment of arbitration with the storage concerned, the information as which the above-mentioned controller expresses the electronic equipment concerned from the electronic equipment concerned is received. If nullification of the electronic equipment concerned is controlled by the information with reference to RIBOKESHON information according to the reference result, it will become possible

to inhibit the record or playback of contents by unjust electronic equipment by the storage side.

[0012] Moreover, except the specific procedure which secured the above-mentioned specific storage region on read-only nonvolatile memory, or was kept secret, if it secures on the rewritable nonvolatile memory which cannot be accessed, management also to the alteration of RIBOKESHON information will be attained.

[0013] In addition, this invention is materialized also as the contents protection approach which used the storage of the above-mentioned configuration.

[0014]

[Embodiment of the Invention] Hereafter, with reference to a drawing, it explains per gestalt of operation of this invention.

[0015] Drawing 1 shows the example of a configuration of the contents use managerial system 1 concerning 1 operation gestalt of this invention. In addition, although music data are used as an example as contents (digital content), you may be ******, a movie, and data, such as game software, in this case here.

[0016] EMD (Electronic Music Distributor) is a music distribution server or a music distribution broadcasting station.

[0017] The contents use managerial system (LCM (Licence Compliant Module (SDMI-)) is called hereafter) 1 is realized using a personal computer (PC). The approach of the contents protection in this LCM1 is premised on managing encryption/decryption of contents using the identification information (media ID) of those storage media every storage media (storage) 13 which should record contents.

[0018] LCM1 has receive section #1-#3 corresponding to two or more EMD(s) (here EMD#1-# 3), and receives the encryption contents which EMD distributes through the receive section #1-#3 concerned, or its license (use conditions and encryption contents decode key). Receive section #1-#3 may have the regenerative function and the accounting function. Moreover, it is possible to purchase the contents included in mind using an accounting function.

[0019] LCM1 has the secure contents server (here, it is Secure Music Server:SMS and Following SMS is called) 2. This SMS2 receives the encryption contents which the user purchased via the EMDI/F (interface) section 3. Encryption contents (here music content) are decoded in the EMDI/F section 3 if needed, and formal conversion and re-encryption are given. If encryption contents are received, SMS2 stores it in the music data storage section 10, and stores a music data decode key (contents decode key) in the license storing section 9. SMS2 may have the regenerative function, in order that a user may try listening the distributed music content, and it can reproduce

on PC the music content which SMS2 manages in this case here.

[0020] SMS2 has the function which outputs contents data (digital content) by the I/F section 6 course concerned again to the storage media (PM (Portable Memory) is called hereafter) 13, such as a memory card with which the media I/F section 6 can be equipped. This PM13 can reproduce the contents recorded on PM13 concerned by setting and using for the record regenerative apparatus (PD (Portable Device) being called simply hereafter) 12 of dedication of the configuration shown in drawing 2 on PD12.

[0021] Record of the contents from SMS2 to PM13 is directly performed through the media I/F section 6, or it can carry out via PD12.

[0022] Here, check-in/check-out function by LCM1 is explained briefly. Check-out means LMS1 storing the contents as "parents" and copying the duplicate to PM13 as "child" contents. Although "child" contents can be fundamentally reproduced freely by PD12, creating "grandchild" contents from a "child" is not allowed. It is defined as an attribute of "parents" how many "parents" can bear a "child." Moreover, check-in is that equip the media I/F section 6 of LCM1 with PM13, and LCM1 eliminates "child" contents (or use impossible), and it says that the "parent" contents in LCM1 recover the right which makes one a "child." This is referred to as checking in at "parents."

[0023] PM13 consists of a controller 130 and the storage media section which consists of a open field 131 and a secrecy field 134, as shown in drawing 3 . The secrecy field 134 is a storage region which can be accessed only in a secret procedure (that is, specific procedure kept secret) through a controller 130, and is used for memorizing information required for contents decode. The secrecy field 134 consists of a secrecy ROM field where constants, such as the media identification information (a media key is called hereafter) KM of a proper, are memorized by corresponding PM13, and a secrecy R/W (read/write) field where variables, such as a license decode key which is restricted data offered from the side to which it licenses (called a media mark), are memorized. If the media key KM is peculiar to each PM13, it is good and a serial number, a serial number (the serial number or manufacture lot number of PM13 each), and other various identification information can be used for it. In addition, you may make it generate the media key KM from identification information peculiar to each PM13, and a license decode key. A secrecy ROM field is secured for example, on ROM (read-only nonvolatile memory), and a secrecy R/W field is secured in the specific region of a flash memory (rewritable nonvolatile memory).

[0024] In the usual procedures other than a secrecy field, the open field 131 is an accessible field and consists of a read-only open field (a open ROM field is called

hereafter) 132 and a rewritable open field (a open R/W field is called hereafter) 133. A open ROM field is secured for example, on ROM, and a open R/W field is secured for example, on a flash memory. This open ROM field and a open R/W field may be made to be secured on ROM from which a previous secrecy ROM field is secured, and the flash memory from which a secrecy R/W field is secured, respectively.

[0025] It registers with the open ROM field 132 beforehand in the shipment phase of PM13 where the RIBOKESHON information related to this invention corresponds directly. This RIBOKESHON information is the information which can distinguish the device (LCM, PD) which should cancel the access request for the device (LCM, PD) which should cancel use of PM13 for protection of contents, record of the digital content for PM13 (inner open R/W field 133) if it states still more concretely, or playback. In this operation gestalt, RIBOKESHON information is the list of the identification information (device ID) of the device which should be cancelled. So, in the following explanation, the vocabulary which it "RIBOKESHON list RL" Comes to replace with "RIBOKESHON information" is used. That is, the RIBOKESHON list RL is beforehand registered into the open ROM field 132.

[0026] In the open R/W field 133, the enciphered contents key (contents decode key), the enciphered contents are memorized suitably. The enciphered contents key is acquired by enciphering the contents (it being proper to contents C concerned) key KC for decoding Contents C by the media key KM depending on PM13. Moreover, the enciphered contents (contents enciphered by the duplex here) are acquired by what (KM [KC[C]]) the contents (KC [C]) enciphered by KC are enciphered for by the media key KM depending on PM13.

[0027] LCM1 and PD12 have the same storage region as PM13, as shown in drawing 4. That is, LCM1 has each storage region of the open field 111 which consists of a open ROM field 112 and a open R/W field 113, and the secrecy field 114 which can be accessed only in a secret procedure. The music data storage section 10 shown in drawing 1 is secured in the open R/W field 113. In the secrecy field 114, the identification information (device ID) IDLCM of LCM1 is memorized beforehand. In the secrecy field 114, the contents key KC for every contents is memorized suitably again. The guest book storing section 8 shown in drawing 1 is further secured in the secrecy field 114. All the music contents held in the music data storage section 10 (open R/W field 113) under management of SMS2 have the number of contents which was beforehand determined as the content ID (TID) which is the identification information and which can be reproduced, i.e., a child's number of **, and a check-out list as the attribute information. This attribute information is stored by a guest book, a call, and

the guest book storing section (inside of the secrecy field 114) 8. LCM1 has the secrecy field driver 7 for reading data in the guest book storing section 8 (secrecy field 114 to offer), after the specific procedure from which it was kept secret for accessing this guest book storing section 8 by SMS2 is performed. In addition, since this guest book is not directly related to this invention, it omits explanation about the detail of that usage.

[0028] On the other hand, PD12 has each storage region of the open field 121 which consists of a open ROM field 122 and a open R/W field 123, and the secrecy field 124 which can be accessed only in a secret procedure. Fixed storage of the identification information IDPD of PD12 is beforehand carried out to the secrecy field 124. In the secrecy field 124, the contents key KC for every contents is memorized suitably again.

[0029] Drawing 2 shows the example of a configuration of PD12. PM13 is equipped with and used for 12f of media I/F sections of PD12. When reading and LCM1 write to PM13 through PD12, the secrecy field 134 (refer to drawing 3 ) of PM13 concerned is accessed via LCMI/F section 12in PDI/F section [ in LCM1 ] 5, and PD12 e, and 12f of media I/F sections. 12f of media I/F sections has the secrecy field access section (not shown) for accessing the secrecy field 134 of PM13. The open R/W field 123 and the secrecy field 124 (refer to drawing 4 ) in PD12 are secured for example, on flash memory 12d. Moreover, the open ROM field 122 (refer to drawing 4 ) is secured on ROM12c. The program for performing mutual recognition between PM13 is written in this ROM12c. In PD12, processing of the mutual recognition between PM13 etc. is performed according to the basis of control of CPU12a, and this program.

[0030] Next, after receiving the enciphered music content which was distributed from EMD in the EMDI/F section 3 of LCM1 and carrying out a temporary storage to the music data storage section 10 by SMS2 about actuation of this operation gestalt, the actuation at the time of the check-out recorded on PM13 with which the media I/F section 6 was equipped by making the "reproduction" into "child" contents (copy) is explained to an example with reference to the flow chart of drawing 5 .

[0031] In this case, mutual recognition of common knowledge between the media I/F section 6 of LCM1 and the controller 130 of PM13 is performed in the phase where directions of check-out were made through the user interface (I/F) section 15 of LCM1, and the media I/F section 6 of LCM1 was equipped with PM13 (step S101). If devices A and PM13 are used as Device B for LCM1, as for this mutual recognition, it is common to be carried out as follows.

[0032] First, Device B shall be attested from Device A. Device A holds the public key kp, and if Device B is sharing the predetermined contents protection feature between

Devices A, it will hold the private key ks corresponding to a public key kp here. Device A generates a random number R and sends it to Device B. If the random number R generated by Device A is received, Device B will encipher it with a private key ks, and will return the enciphered random number (it expresses ks [R]) to Device A. By Device A, ks [R] is decoded using a public key kp, and if a decode result is equal to the random number R generated previously, it will judge with Device B being a right partner.

[0033] Then, mutual recognition can be performed by performing the same thing as the above from Device B to Device A. In this case, Device B holds a public key and it checks whether it is equal to the random number which Device A held the private key, enciphered the random number which Device A generated by Device B with the private key, decoded it using the public key by Device B, and was generated previously.

[0034] When it is checked by the above mutual recognition (S101) that he is a partner just on the both sides of LCM1 and PM13, key exchange is performed between the media I/F section 6 of LCM1, and the controller 130 of PM13, and the same authentication key (KX1) is shared. This key exchange is performed by the approach using the random challenge response represented by CSS (Content Scrambling System) currently used as contents encryption algorithm of DVD-ROM. An authentication key (KX1) is a strange key when replacing each time.

[0035] The media I/F section 6 of LCM1 reads the identification information IDLCM of the self currently kept secret from the secrecy field 114 (storage), enciphers the IDLCM concerned with an authentication key (KX1), and sends the enciphered IDLCM (= KX1 [IDLCM]) to PM13 from the media I/F section 6 (step S102).

[0036] The controller 130 of PM13 decodes KX1 from the LCM1 side [IDLCM] with the authentication key (KX1) acquired by previous key exchange, and obtains IDLCM (step S103). Next, the controller 130 of PM13 judges whether use of PM13 by LCM1 is cancelled by whether the identification information which is in agreement with the IDLCM concerned with the identification information IDLCM of decoded LCM1 with reference to the RIBOKESHON list RL of [ in the open ROM field 132 ] is registered (step S104).

[0037] When the identification information which is in agreement with IDLCM is registered into the RIBOKESHON list RL, a controller 130 is judged to be what should cancel use of PM13 by corresponding LCM1 (RIBOKETO), and suspends subsequent processings.

[0038] On the other hand, when the identification information which is in agreement with IDLCM is not registered into the RIBOKESHON list RL, a controller 130 is judged

to be what use of PM13 by corresponding LCM1 is permitted, and reads and outputs the media key KM currently kept secret from the secrecy field 134 (step S105). and after performing key (minding the media I/F section 6 of LCM1 concerned) exchange between the media I/F sections 6 of LCM1 and sharing the same authentication key (KX2), a controller 130 enciphers the media key KM which carried out [ above-mentioned ] reading appearance with an authentication key (KX2), and sends the enciphered KM (= KX2 [KM]) to LCM1 (step S106).

[0039] The media I/F section 6 of LCM1 decodes KX2 from the PM13 side [KM] with the authentication key (KX2) acquired by previous key exchange, and obtains the media key KM (step S107). Next, it enciphers by the media key KM which acquired the contents key KC currently kept secret from the secrecy field 114, and the media I/F section 6 of LCM1 writes the enciphered KC (= KM [KC]) in the open R/W field 133 of PM13 (step S108).

[0040] Thus, LCM1 receives the media key KM which will not be passed from PM13 if cancelled according to the RIBOKESHON list RL (RIBOKETO) (enciphered) from PM13 concerned, and he enciphers the contents key KC currently kept secret from the secrecy field 114 of the LCM1 by the media key KM concerned, and is trying to write in the open R/W field 133 of PM13 with this operation gestalt. For this reason, an authentication key is exchanged between LCM1 and PM13, and the candidate LCM for nullification (electronic equipment which is going to use PM13) specified by the RIBOKESHON list RL can be certainly cancelled compared with the approach of performing encryption/decryption of a contents key using that recognition key (exclusion). In addition, in case the encryption contents (KC [C]) accumulated in the music data storage section 10 secured in the open R/W field 113 of LCM1 are sent to PM13, you may make it encipher further by KM which carried out [ above-mentioned ] acquisition.

[0041] Next, the actuation in the case of decoding the encryption contents stored in PM13 on PD12, and reproducing is explained with reference to the flow chart of drawing 6 . First, mutual recognition (it is the same as that of said step S101) is performed between CPU12a of PD12, and the controller 130 of PM13 in the phase where reproductive directions were made to PD12, and 12f of media I/F sections of PD12 was equipped with PM13 (step S201). and the time of it being checked by this mutual recognition (S201) that he is a partner just on the both sides of PD12 and PM13 -- CPU12 of PD12 -- key exchange is performed between the controllers 130 of a and PM13, and the same authentication key (KX3) is shared.

[0042] CPU12a of PD12 reads the identification information IDPD of the self currently

kept secret from the secrecy field 124, enciphers the IDPD concerned with an authentication key (KX3), and sends the enciphered IDPD (= KX3 [IDPD]) to PM13 from 12f of media I/F sections (step S202).

[0043] The controller 130 of PM13 decodes KX3 from the PD12 side [IDPD] with the authentication key (KX3) acquired by previous key exchange, and obtains IDPD (step S203). Next, the controller 130 of PM13 judges whether use of PM13 by PD12 is cancelled by whether the identification information which is in agreement with the IDPD concerned with the identification information IDPD of decoded PD12 with reference to the RIBOKESHON list RL of [ in the open ROM field 132 ] is registered (step S204).

[0044] When the identification information which is in agreement with IDPD is registered into the RIBOKESHON list RL, a controller 130 is judged to be what should cancel use of PM13 by corresponding PD12 (RIBOKETO), and suspends subsequent processings.

[0045] On the other hand, when the identification information which is in agreement with IDPD is not registered into the RIBOKESHON list RL, a controller 130 is judged to be what use of PM13 by corresponding PD12 is permitted, and reads and outputs the media key KM currently kept secret from the secrecy field 134 (step S205). and after performing key (minding 12f of media I/F sections of PD12 concerned) exchange between CPU12a of PD12 and sharing the same authentication key (KX4), a controller 130 enciphers the media key KM which carried out [ above-mentioned ] reading appearance with an authentication key (KX4), and sends the enciphered KM (= KX4 [KM]) to PD12 (step S206).

[0046] CPU12a of PD12 decodes KX4 from the PM13 side [KM] with the authentication key (KX4) acquired by previous key exchange, and obtains the media key KM (step S207). Next, CPU12a of PD12 reads the enciphered contents key KC (= KM [KC]) which is memorized to the open R/W field 133 of PM13, decodes it by the media key KM acquired at step S207, writes the decoded contents key KC in the secrecy field 124, and secrecy-izes it (step S208). Therefore, in PD12, it becomes possible to decode the encryption contents memorized to the open R/W field 133 of PM13, and to reproduce using this decoded contents Key KC (media key KM previously decrypted when required).

[0047] Thus, PD12 receives the media key KM which will not be passed from PM13 if cancelled according to the RIBOKESHON list RL (RIBOKETO) (enciphered) from PM13 concerned, and he decrypts the encryption contents key (KM [KC]) currently kept secret from the secrecy field 134 of PM13 concerned by the media key KM, and

is trying to write it in the secrecy field 124 of PD12 with this operation gestalt. For this reason, an authentication key is exchanged between PD12 and PM13, and the candidate PD for nullification (electronic equipment which is going to use PM13) specified by the RIBOKESHON list RL can be certainly cancelled compared with decrypting an encryption contents key using that recognition key.

[0048] In addition, although the information concerned shall be enciphered with an authentication key (KXi) in case information currently kept secret from the secrecy field or information which should be kept secret from a secrecy field is delivered and received between LCM1 and PM13 and between PD12 and PM13, the encryption with an authentication key is not necessarily required of the above operation gestalt. However, in order to make contents protection into a more positive thing, it is desirable to perform encryption with an authentication key.

[0049] Moreover, although the above operation gestalt explained as that by which the RIBOKESHON list RL is registered into the open ROM field 132, you may make it register with the secrecy field 134 which can be accessed only in the specific procedure kept secret that what is necessary is just the field where the RIBOKESHON list RL is not altered.

[0050]

[Effect of the Invention] When the storage concerned uses it for the specific storage region of a storage on the electronic equipment with which it is expressed by the above-mentioned list according to this invention, equipping since the RIBOKESHON information which can distinguish the electronic equipment which should be cancelled for contents protection considered as the configuration registered beforehand as explained in full detail above, the electronic equipment can be cancelled and protection of contents can be aimed at.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block block diagram of the contents use managerial system concerning 1 operation gestalt of this invention.

[Drawing 2] The block block diagram of PD12 in drawing 1 (record regenerative apparatus).

[Drawing 3] The block block diagram of PM13 in drawing 1 (storage media).

[Drawing 4] Drawing showing the example of a storage region configuration of LCM1 and PD12.

[Drawing 5] Drawing for explaining the operations sequence at the time of the contents record to PM13 from LCM1.

[Drawing 6] Drawing for explaining the operations sequence in the case of decoding the encryption contents stored in PM13 on PD12, and reproducing.

[Description of Notations]

1 -- LCM (contents use managerial system)

2 -- SMS (secure contents server)

5 -- PDI/F section

6 -- Media I/F section

7 -- Secrecy field driver

8 -- Guest book storing section

9 -- License storing section

10 -- Music data storage section

11 -- CDI/F section

12 -- PD (record regenerative apparatus)

13 -- PM (a storage, storage media)

112,122,132 -- Open ROM field

113,123,133 -- Open R/W field

114,124,134 -- Secrecy field

130 -- Controller